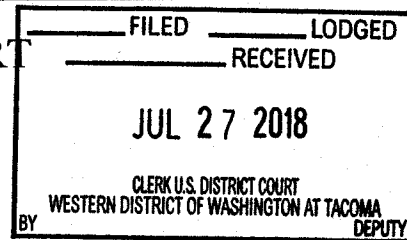


UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)THE PERSON OF KENNETH CURRIN SCHUCHMAN,
AS FURTHER DESCRIBED IN ATTACHMENT A

Case No.

MJ18-5187

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

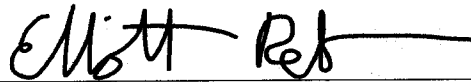
Code Section
 18 USC 1030
 18 USC 1343

Offense Description
 Unauthorized Damage to a Protected Computer
 Wire Fraud

The application is based on these facts:

See Attached Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

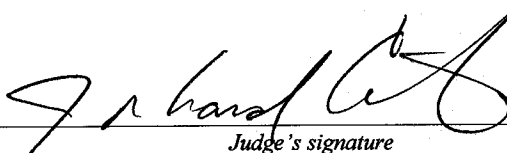
Elliott Peterson, Special Agent

Sworn to before me pursuant to CrimRule 4.1.

Date:

7/27/18

City and state: Tacoma, Washington



Judge's signature

J. Richard Creatura, United States Magistrate Judge

Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
 COUNTY OF PIERCE)

I, **Elliott Peterson**, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation, and have been so employed since 2011. I am currently assigned within the Anchorage Field Office to the Counter Intelligence / Cyber Squad. I perform and have performed a variety of investigative tasks, including functioning as a case agent on computer crime cases. Since becoming a Special Agent of the FBI, I have received many hours of specialized cyber training, including on the topic of computer networking. I have also received training and gained experience in interviewing and interrogation techniques, the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence. I specialize in the investigation of botnets, Distributed Denial of Service (DDOS), and embedded devices, also known as the "Internet of Things" (IoT).

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search of the person of KENNETH CURRIN SCHUCHMAN within the Western District of Washington, hereinafter the "SUBJECT," as more fully described in Attachment A to this Affidavit, for the property and items described in Attachment B to this Affidavit. Because I work out of the Anchorage Field Office, and due to the technical nature of the evidence described below, I request that I be allowed to present this application by telephone pursuant to Local Criminal Rule 41(d)(3). In compliance with Local Criminal Rule 41, this application has been reviewed by Francis Franze-Nakamura who is an Assistant United States Attorney for the Western District of Washington.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this

1 investigation, including other law enforcement officers; interviews of cooperating
 2 witnesses; review of documents and records related to this investigation; communications
 3 with others who have personal knowledge of the events and circumstances described
 4 herein; and information gained through my training and experience.

5 4. Because this Affidavit is submitted for the limited purpose of establishing
 6 probable cause in support of the application for a search warrant, it does not set forth
 7 each and every fact that I or others have learned during the course of this investigation. I
 8 have set forth only the facts that I believe are necessary to establish probable cause to
 9 believe that evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 1030
 10 (unauthorized damage to a protected computer) and 1343 (wire fraud) have been
 11 committed by the SUBJECT by means of digital devices on his person or in his
 12 immediate control.

13 **THE INVESTIGATION**

14 5. The FBI is currently investigating the SUBJECT of this search warrant
 15 application, KENNETH SCHUCHMAN (a.k.a. "Nexus"), and his co-conspirators Aaron
 16 Sterritt (a.k.a. "Vamp") and Logan Shwydiuk (a.k.a. "Drake"), and their respective roles
 17 in the development and employment of successor variants of the Mirai botnet known as
 18 "Nexus_Mirai," "Satori," and "Masuta." These botnets have infected hundreds of
 19 thousands of devices, including devices within the United States. The Nexus_Mirai
 20 botnet has infected devices within the District of Alaska and the Western District of
 21 Washington. Devices located within the District of Alaska have been forced to
 22 participate in Nexus_Mirai DDOS attacks, as described below. These botnets have been
 23 utilized to conduct DDOS attacks against targets within the United States.

24 *Cooperating Witness 1*

25 6. Since October 2016, the FBI has been investigating the progenitor Mirai
 26 botnet. The Mirai botnet was used in the summer and fall of 2016 to conduct massive
 27 DDOS attacks, sufficient in duration and intensity to cause significant damage to some of
 28 the world's largest Internet Service Providers (ISPs). Even companies who specialize in

1 DDOS defense incurred significant monetary losses as a result of Mirai-based DDOS
2 attacks. At its peak, the botnet consisted of more than 300,000 compromised computing
3 devices. The Mirai botnet targeted IoT devices. Examples of IoT devices targeted by
4 Mirai include internet-connected closed circuit TV cameras and digital video recorders.

5 7. The FBI's investigation into the Mirai botnet led to the establishment of
6 multiple cooperating witnesses. One of the Mirai co-conspirators, Cooperating Witness 1
7 (CW1), has agreed to assist the government in its ongoing Nexus_Mirai and Masuta
8 investigations.

9 8. CW1 is assisting the government pursuant to a plea agreement that provides
10 CW1, along with his co-defendants, the opportunity to argue for a reduced sentence if
11 CW1 is shown to have provided substantial assistance in ongoing investigations. CW1
12 has been cooperating since July 2017. Both of his co-defendants began cooperating
13 shortly thereafter.

14 9. During this period of cooperation, I have found CW1 to be detailed and
15 honest in his production of information. He has no prior criminal history. CW1 is well-
16 versed in matters concerning IoT botnets and DDOS attacks. CW1 also has an expert
17 understanding of many computer science and programming matters. While cooperating,
18 CW1 has sought additional training in programming and topics relevant to his continued
19 assistance of the government. I have been able to independently corroborate the
20 information provided to the government by CW1, either by consulting with industry
21 experts or other cooperating witnesses, or by comparing CW1's data to data produced
22 through other mechanisms such as grand jury subpoenas, or because the provided data
23 was in an audio or video format, and reviewable in its entirety.

24 *Criminal Organization*

25 10. Based upon the work of CW1, as well as independent investigation, I know
26 that the Nexus_Mirai botnet was operated primarily by the SUBJECT beginning in
27 November 2017, and continuing in various forms to the present. The Masuta and Satori
28 variants were developed and operated by the SUBJECT, Sterritt, Shwydiuk and others

1 still unidentified. For the purpose of clarity, I understand both Masuta and Satori to be
2 Mirai variants that predominantly utilize a code base principally developed by Sterritt
3 (“Vamp”). This is in contrast to the Nexus_Mirai variant which I understand to be
4 principally developed by the SUBJECT. For simplicity, I will refer to the Masuta and
5 Satori family of variants simply as Masuta for the remainder of the affidavit.

6 11. The SUBJECT utilizes the nickname “Nexus” and resided until recently at
7 his grandmother’s residence in the Vancouver, Washington area. At this time, however,
8 the SUBJECT does not have a stable residence or predictable lodging.

9 12. The SUBJECT’s co-conspirator, Sterritt, principally utilizes the nickname
10 “Vamp” and is known to reside in Northern Ireland. The third co-conspirator, Shwydiuk,
11 utilizes the nickname “Drake” and is a resident of Canada. The SUBJECT, Sterritt, and
12 Shwydiuk all are well known to law enforcement, and have engaged in many online
13 crime schemes over the years, although I am only investigating their assembly of botnets
14 for the purpose of conducting DDOS attacks.

15 13. I have reviewed audio and video conversations, recorded by CW1, between
16 the SUBJECT, Shwydiuk, and Sterritt, in which they discuss their ongoing schemes and
17 refer to each other by their online nicknames. For example, in one such chat on
18 November 22, 2017, the SUBJECT, Sterritt, and others discuss the development of the
19 botnet. In particular, they discuss programming languages and methods that are being
20 used to improve the botnet. Their discussion of the attacks also referenced “NineGigs,”
21 which I know to be a reference to the online nickname of an employee at the DDOS
22 defense company ProxyPipe.

23 14. As part of this investigation I have interviewed an employee of the
24 ProxyPipe company. According to the employee, ProxyPipe has been targeted multiple
25 times by the Masuta botnet, starting in November 2017. ProxyPipe is a U.S. company.

26 15. CW1 has communicated with the SUBJECT via Skype, a messaging
27 platform, where the SUBJECT uses the Skype handle “TsGH Nexus Zeta.” During a
28 Skype video chat recorded on November 29, 2017, the SUBJECT states, “Me and Vamp

1 literally ran Satori with 100K on a five dollar box and nulled ProxyPipe.” Based upon
2 my training and experience, I know that when the SUBJECT states that he “ran Satori
3 with 100K” he is referencing a DDOS botnet with at least 100,000 infected devices.
4 When the SUBJECT references a “five dollar box,” he is indicating that he hosted the
5 botnet utilizing a very cheap server. Finally, “nulled ProxyPipe” is meant to indicate that
6 the SUBJECT’s botnet conducted a DDOS attack against ProxyPipe and succeeded in
7 disrupting network communications for some time period. During this recorded video
8 chat, the SUBJECT is recognizable by both voice and face. I have reviewed Department
9 of Motor Vehicles (DMV) photographs of the SUBJECT and confirmed that the face
10 from the video chat visually matches the face from the DMV photograph. During this
11 chat, the SUBJECT actually affirmatively states that his name is KENNETH
12 SCHUCHMAN.

13 16. The SUBJECT is also associated with various domains including
14 nexusiotsolutions[.]net, nexuszeta[.]com, and zetastress[.]net. Historically, these
15 domains have been associated with DDOS attacks. The first referenced domain,
16 nexusiotsolutions.net, has been utilized as part of the command and control protocol for
17 the Masuta botnet. This malicious use of the domain has been determined by various
18 security researchers who have observed malware payloads, in which the victim devices
19 are sent instructions referencing the nexusiotsolutions[.]net domain. Essentially, the
20 victim devices are forced to communicate with this domain when they become part of the
21 Masuta botnet.

22 17. I have searched email accounts utilized by the SUBJECT to register or
23 maintain the above domains and services. These email accounts contain many references
24 to his true identity, including copies of government-issued identification cards. One of
25 his email accounts also contains abuse notifications from hosting providers related to the
26 operation of his botnet. This means that he was notified that botnets he was operating
27 had been discovered by Internet security researchers. Within the SUBJECT’s internet
28 search history, I found many references to the Mirai botnet. Similarly, I found many

1 references to IoT credentials, meaning that the SUBJECT was searching for usernames
2 and passwords that could be used to access IoT devices, the type of devices upon which
3 his botnet was built. Based upon my investigation I have concluded that the SUBJECT is
4 the individual also known as "Nexus" who has operated the Nexus_Mirai botnet using
5 digital devices within his possession and control as instrumentalities of the subject
6 offenses.

7 18. The SUBJECT has had an unsteady relationship with Sterritt, which is
8 relatively common for cybercriminals. Based upon conversations with CW1, and
9 conversations that CW1 has recorded with both the SUBJECT and Sterritt, it appears that
10 they frequently disagree. For example, according to CW1, approximately two months
11 ago Sterritt came to the conclusion that the SUBJECT was cooperating with law
12 enforcement and cut him out of his operation. They have not yet reconciled. I am
13 unaware of any cooperation, past or present, between the SUBJECT and law
14 enforcement.

15 19. I have tracked subject's botnet development through several methods,
16 including focusing on the domains and IP addresses utilized to compromise victim
17 devices and issue attack commands. My investigation has determined that the following
18 IP addresses and domains have been associated with the SUBJECT's command and
19 control of his botnet and DDOS activities: 185.188.206.99, 45.32.238.229, 208.78.71.34,
20 nexusiotsolutions.com, nexuszeta.com, and zetastress.net.

21 20. The SUBJECT's activities have harmed users in Alaska and elsewhere.
22 While the full extent of harm is still being investigated, I have determined that Alaskan
23 devices participated in at least one of Sterritt's DDOS attacks conducted utilizing his
24 Masuta botnet. On August 13, 2017, the Masuta botnet was utilized to attack servers
25 belonging to the U.S. company Take-Two Interactive Software Inc. (Take-Two). I was
26 able to determine that the botnet utilized to conduct this attack was Masuta based upon
27 examining logs relating to attack commands issued from a known Masuta command and
28 control server. This attack targeted an authentication server utilized by Take-Two and

1 prevented the proper functioning of several of their servers. Take-Two has logs relating
2 to the devices which participated in this attack, and at least two separate IPs
3 corresponding to two Alaskan Internet Service Providers appear within this log, meaning
4 that two devices utilizing Alaskan IPs were part of the botnet. This is consistent with
5 previously observed activity from other DDOS botnets such as Mirai and Nexus_Mirai.

6 21. At the time of these attacks, CW1 was frequently in communication with
7 Sterritt. I have reviewed an audio recording of a conversation on August 13, 2017, in
8 which CW1 discusses an attack against Take-Two. I recognize the voice of the other
9 party in the conversation to be Sterritt's. During the conversation, Sterritt discusses that
10 he was able to conduct a successful DDOS attack against Take-Two, by focusing his
11 attack on the authentication server, as was separately indicated in Take-Two's logs of the
12 attacks.

13 22. CW1 has communicated with the SUBJECT frequently via mobile phone,
14 to include text messages. On June 4, 2018, the SUBJECT, using a mobile phone, asked
15 CW1 to create a bitcoin wallet in order to transfer to him proceeds from a "client who
16 wants a spot." I have seen the SUBJECT and others utilize this language previously to
17 describe customers for a botnet. The SUBJECT recently provided CW1 with access to a
18 server that CW1 understands to be utilized by the SUBJECT to actively manage a botnet.

19 23. Pursuant to a search warrant issued in the District of Alaska, I received
20 location data relative to this previously utilized phone number during June and July 2018.
21 That data indicated that the SUBJECT is residing in the Vancouver, Washington area.
22 That data also indicated that the SUBJECT recently switched phone numbers, and is no
23 longer a subscriber for the previously utilized phone number. Based on this recent
24 location data, as well as other information available to law enforcement, the SUBJECT is
25 not believed to have a stable residence at this point.

26 24. CW1 contacted the SUBJECT via a new cell phone number on July 12,
27 2018. On that date, CW1 confirmed with the SUBJECT that he was actively utilizing the
28 cell phone number. CW1 again exchanged text messages with the SUBJECT on July 19,

1 2018, indicating that the SUBJECT is still in active use of the cell phone number. On
2 July 20, 2018, CW1 and the SUBJECT had a telephone conversation regarding
3 Schuchman flying to visit CW1. During this call, the SUBJECT was utilizing the same
4 cell phone number.

5 TECHNICAL TERMS

6 25. Based on my training and experience, I use the following technical terms to
7 convey the following meanings:

8 a. "DDOS" or "DDOS attacks" are distributed denial of service
9 attacks. DDOS attacks are a specific type of cyberattack, in which a perpetrator intends
10 to disrupt services of a server or host on the Internet. Often these attacks are undertaken
11 by flooding a server with numerous requests, causing the server to overload and become
12 unable to respond to incoming traffic. A common example of a DDOS attack would be
13 thousands of simultaneous requests to a webpage, which would cause the webpage to
become inoperable due to the server's inability to accept and respond to all the incoming
traffic.

14 b. A "botnet" is a network of computers communicating together, or
15 controlled by common computers. Cybercriminals often infect victim machines and use
16 them in unison with other infected machines to undertake further coordinated activities
17 such as DDOS attacks. The victim machines under the control of the cybercriminal
18 would be the cybercriminal's "botnet," as they are numerous computers under his/her
19 control. Using the multitude of computers, a cybercriminal could conduct a DDOS attack
by commanding his botnet to attack a single website in unison, causing the website to
become inoperable.

20 c. The "Internet of Things," or IoT, is a classification of embedded
21 devices that are computers pursuant to the definitions relevant to 18 U.S.C. § 1030.
22 These devices commonly run variations of the Linux operating system and are designed
23 around a core set of features. Some examples of IoT devices include internet switches,
routers, DVRs, and surveillance systems, among other devices.

24 d. Mirai is the name of a large DDOS botnet comprised primarily of
25 IoT devices that was developed and deployed in 2016 by a criminal group that did not
26 include the SUBJECT of this investigation or Sterritt. That criminal group subsequently
27 released the code for Mirai publically in 2016 in an unsuccessful effort to avoid
28 apprehension, resulting in many subsequent variants being utilized in later DDOS attack
schemes by other criminal actors.

e. A “Whois” search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.345.67.0– 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0– 12.345.67.99.

f. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. Electronic Storage media: Electronic Storage media is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

26. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, and/or instrumentalities that might be found on the person of the SUBJECT or in his immediate control, in whatever form they are found. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on

1 digital devices¹ such as computer hard drives or other electronic storage media.² Thus,
2 the warrant applied for would authorize the seizure of digital devices or other electronic
3 storage media or, potentially, the copying of electronically stored information from
4 digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

5 27. *Probable cause.* Based upon my review of the evidence gathered in this
6 investigation, my review of data and records, information received from other agents and
7 computer forensics examiners, and my training and experience, I submit that if a digital
8 device or other electronic storage media is found on or in the immediate control of the
9 SUBJECT, there is probable cause to believe that evidence, fruits, and/or
10 instrumentalities of the crimes of 18 U.S.C. §§ 1030 (unauthorized damage to a protected
11 computer) and 1343 (wire fraud) will be stored on those digital devices or other
12 electronic storage media. I believe digital devices, including a cellular phone and laptop
13 computer, are being used to conduct research into vulnerabilities for digital devices later
14 compromised by the SUBJECT in order to increase the size and power of his botnet. I
15 also believe that digital devices are utilized to maintain control over the victim devices of
16 which make up the SUBJECT's botnet, and that these same devices are utilized to issue
17 DDOS attack commands. I would expect to find files, applications, and Internet artifacts
18 on the SUBJECT's digital devices that relate to his aforementioned botnet activities.
19 This expectation is further reinforced by searches executed upon the SUBJECT's email
20 accounts in which such artifacts were located. There is, therefore, probable cause to
21

22 ¹ "Digital device" includes any device capable of processing and/or storing data in electronic form,
23 including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers,
24 computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters,
25 monitors, and drives intended for removable media, related communications devices such as modems,
26 routers and switches, and electronic/digital security devices, wireless communication devices such as
mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"),
iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices
(GPS), or portable media players.

27 ² Electronic Storage media is any physical object upon which electronically stored information can be
28 recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other
magnetic or optical media.

1 believe that evidence, fruits and/or instrumentalities of the crimes of 18 U.S.C. §§ 1030
2 (unauthorized damage to a protected computer) and 1343 (wire fraud) exists and will be
3 found on digital device or other electronic storage media on the person of the SUBJECT
4 or in his immediate control, for at least the following reasons:

5 a. Based on my knowledge, training, and experience, I know that
6 computer files or remnants of such files can be preserved (and consequently also then
7 recovered) for months or even years after they have been downloaded onto a storage
8 medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a
9 digital device or other electronic storage medium can be stored for years at little or no
10 cost. Even when files have been deleted, they can be recovered months or years later
11 using forensic tools. This is so because when a person “deletes” a file on a digital device
or other electronic storage media, the data contained in the file does not actually
disappear; rather, that data remains on the storage medium until it is overwritten by new
data.

12 b. Therefore, deleted files, or remnants of deleted files, may reside in
13 free space or slack space—that is, in space on the digital device or other electronic
14 storage medium that is not currently being used by an active file—for long periods of
15 time before they are overwritten. In addition, a computer’s operating system may also
keep a record of deleted data in a “swap” or “recovery” file.

16 c. Wholly apart from user-generated files, computer storage media—in
17 particular, computers’ internal hard drives—contain electronic evidence of how a
18 computer has been used, what it has been used for, and who has used it. To give a few
19 examples, this forensic evidence can take the form of operating system configurations,
20 artifacts from operating system or application operation; file system data structures, and
21 virtual memory “swap” or paging files. Computer users typically do not erase or delete
this evidence, because special software is typically required for that task. However, it is
technically possible to delete this information.

22 d. Similarly, files that have been viewed via the Internet are sometimes
23 automatically downloaded into a temporary Internet directory or “cache.”

24 28. As discussed in greater detail above, the SUBJECT uses digital devices in
25 his personal possession to research, maintain, and conduct DDOS attacks in violation of
26 18 U.S.C. § 1030. The creation of botnets in order to execute DDOS attacks upon third
27 parties is predicated upon the compromise of victim IoT devices such as home internet
28 routers. Previous examination of the SUBJECT’s internet search history and email

1 accounts, as authorized by previously issued search warrants in the District of Alaska,
2 have revealed the SUBECT has used his personal digital devices to research methods for
3 the creation, control, and deployment of sophisticated IoT botnets. As a result, these
4 personal digital devices are expected to be permeated with evidence of these crimes and
5 were used primarily during the period in question as instrumentalities of these offenses.

6 29. *Forensic evidence.* As further described in Attachment B, this application
7 seeks permission to locate not only computer files that might serve as direct evidence of
8 the crimes described on the warrant, but also forensic electronic evidence that establishes
9 how digital devices or other electronic storage media were used, the purpose of their use,
10 who used them, and when. There is probable cause to believe that this forensic electronic
11 evidence will be on any digital devices or other electronic storage media located on the
12 person of the SUBJECT or in his immediate control because:

13 a. Stored data can provide evidence of a file that was once on the
14 digital device or other electronic storage media but has since been deleted or edited, or of
15 a deleted portion of a file (such as a paragraph that has been deleted from a word
16 processing file). Virtual memory paging systems can leave traces of information on the
17 digital device or other electronic storage media that show what tasks and processes were
18 recently active. Web browsers, e-mail programs, and chat programs store configuration
19 information that can reveal information such as online nicknames and passwords.
20 Operating systems can record additional information, such as the history of connections
21 to other computers, the attachment of peripherals, the attachment of USB flash storage
22 devices or other external storage media, and the times the digital device or other
23 electronic storage media was in use. Computer file systems can record information about
24 the dates files were created and the sequence in which they were created.

25 b. As explained herein, information stored within a computer and other
26 electronic storage media may provide crucial evidence of the “who, what, why, when,
27 where, and how” of the criminal conduct under investigation, thus enabling the United
28 States to establish and prove each element or alternatively, to exclude the innocent from
further suspicion. In my training and experience, information stored within a computer
or storage media (e.g., registry information, communications, images and movies,
transactional information, records of session times and durations, internet history, and
anti-virus, spyware, and malware detection programs) can indicate who has used or
controlled the computer or storage media. This “user attribution” evidence is analogous
to the search for “indicia of occupancy” while executing a search warrant at a residence.
The existence or absence of anti-virus, spyware, and malware detection programs may

1 indicate whether the computer was remotely accessed, thus inculcating or exculpating the
2 computer owner and/or others with direct physical access to the computer. Further,
3 computer and storage media activity can indicate how and when the computer or storage
4 media was accessed or used. For example, as described herein, computers typically
5 contain information that log: computer user account session times and durations,
6 computer activity associated with user accounts, electronic storage media that connected
7 with the computer, and the IP addresses through which the computer accessed networks
8 and the internet. Such information allows investigators to understand the chronological
9 context of computer or electronic storage media access, use, and events relating to the
10 crime under investigation.¹ Additionally, some information stored within a computer or
11 electronic storage media may provide crucial evidence relating to the physical location of
12 other evidence and the suspect. For example, images stored on a computer may both
13 show a particular location and have geolocation information incorporated into its file
14 data. Such file data typically also contains information indicating when the file or image
15 was created. The existence of such image files, along with external device connection
16 logs, may also indicate the presence of additional electronic storage media (e.g., a digital
17 camera or cellular phone with an incorporated camera). The geographic and timeline
18 information described herein may either inculcate or exculpate the computer user. Last,
19 information stored within a computer may provide relevant insight into the computer
20 user's state of mind as it relates to the offense under investigation. For example,
21 information within the computer may indicate the owner's motive and intent to commit a
22 crime (e.g., internet searches indicating criminal planning), or consciousness of guilt
23 (e.g., running a "wiping" program to destroy evidence on the computer or password
24 protecting/encrypting such evidence in an effort to conceal it from law enforcement).

25
26 c. A person with appropriate familiarity with how a digital device or
27 other electronic storage media works can, after examining this forensic evidence in its
28 proper context, draw conclusions about how the digital device or other electronic storage
media were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries,
logs, or other forms of forensic evidence on a digital device or other electronic storage
media that are necessary to draw an accurate conclusion is a dynamic process. While it is
possible to specify in advance the records to be sought, digital evidence is not always
data that can be merely reviewed by a review team and passed along to investigators.
Whether data stored on a computer is evidence may depend on other information stored

¹ For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer
used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet
browser was used to download child pornography; and c) at 11:05 am the internet browser was used to
log into a social media account in the name of John Doe, an investigator may reasonably draw an
inference that John Doe downloaded child pornography.

1 on the computer and the application of knowledge about how a computer behaves.
 2 Therefore, contextual information necessary to understand other evidence also falls
 3 within the scope of the warrant.

4 e. Further, in finding evidence of how a digital device or other
 5 electronic storage media was used, the purpose of its use, who used it, and when,
 6 sometimes it is necessary to establish that a particular thing is not present. For example,
 7 the presence or absence of counter-forensic programs or anti-virus programs (and
 8 associated data) may be relevant to establishing the user's intent.

9 **DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES**

10 30. As discussed above, the investigation has determined that the SUBJECT
 11 has used his personal digital devices to research, develop, maintain and deploy
 12 sophisticated IoT botnets for the purposes of committing offenses under the Computer
 13 Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* Investigation into the SUBJECT's life
 14 has determined that the SUBJECT's primary "occupation" is the criminal activities
 15 described above. The SUBJECT does not appear to be lawfully employed or have any
 16 other legitimate source of income at this time other than his criminal activities.

17 **PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION**

18 31. Several other subpoenas and search warrants have issued to date in this
 19 matter for the review of electronically stored information regarding the SUBJECT's
 20 activities. The United States has applied for, received, and served several search warrants
 21 to Google, Inc., for both content and non-content account information associated with the
 22 SUBJECT, including the DDOS botnet search history described above. Those warrants
 23 also included emails containing the registration of domains associated with the operation
 24 of botnets and the notification of abuse complaints related to those domains. The
 25 presence of such messages indicates these devices are utilized extensively to facilitate the
 26 SUBJECT's botnet activities

27 32. Because of the nature of the evidence that I am attempting to obtain and the
 28 nature of the investigation, I have not made any prior efforts to obtain the evidence based
 on the consent of any party who may have authority to consent. I believe, based upon the
 nature of the investigation and the information I have received, that if the SUBJECT

1 becomes aware of the investigation in advance of the execution of a search warrant, he
2 may attempt to destroy any potential evidence, whether digital or non-digital, thereby
3 hindering law enforcement agents from the furtherance of the criminal investigation.

4 **RISK OF DESTRUCTION OF EVIDENCE**

5 33. I know based on my training and experience that digital information can be
6 very fragile and easily destroyed. Digital information can also be easily encrypted or
7 obfuscated such that review of the evidence would be extremely difficult, and in some
8 cases impossible. In the instant case, I know that the SUBJECT is familiar with basic and
9 advanced tenets of computer security. Accordingly I believe subject will utilize practices
10 such as the encryption of storage devices for his digital devices, as well as the usage of
11 encrypted communication programs and protocols. With such systems, if the digital
12 device is either powered off or if the user has not entered the encryption password and
13 logged onto the computer, it is likely that any information contained on the computer will
14 be impossible to decipher. If the computer is powered on, however, and the user is
15 already logged onto the computer, there is a much greater chance that the digital
16 information can be extracted from the computer. This is because when the computer is
17 on and in use, the password has already been entered and the data on the computer is
18 accessible. However, giving the owner of the computer time to activate a digital security
19 measure, pull the power cord from the computer, or even log off of the computer could
20 result in a loss of digital information that could otherwise have been extracted from the
21 computer.

22 **REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET**
23 **COMPUTERS**

24 34. *Necessity of seizing or copying entire computers or storage media.* In most
25 cases, a thorough search of premises for information that might be stored on digital
26 devices or other electronic storage media often requires the seizure of the physical items
27 and later off-site review consistent with the warrant. In lieu of removing all of these
28 items from the premises, it is sometimes possible to make an image copy of the data on

the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

SEARCH TECHNIQUES

35. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of

1 Attachment B to this Affidavit, and will specifically authorize a later review of the media
2 or information consistent with the warrant.

3 36. The United States is seeking authorization to search devices under the
4 exclusive dominion and control of the SUBJECT. As a result of the fact that the
5 SUBJECT does not appear to have a fixed residence, the United States is planning to
6 approach the subject at a neutral location while the subject is conversing with CW1. The
7 SUBJECT has requested to meet with CW1 in person in order to discuss criminal botnet
8 activity, among other subjects. The United States has previously applied for and received
9 search warrants permitting the real time "ping" of cellular devices used by the SUBJECT
10 in order to ascertain his location. Pursuant to this application, the United States seeks
11 only to search the SUBJECT for his own devices in his immediate possession and search
12 those devices for evidence of the crimes described above. As a result of the planned
13 search, there is little to no risk that any device other than those used by the SUBJECT
14 will be examined.

15 37. Consistent with the above, I hereby request the Court's permission to seize
16 and/or obtain a forensic image of digital devices or other electronic storage media that
17 reasonably appear capable of containing data or items that fall within the scope of
18 Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or
19 other electronic storage media and/or forensic images, using the following procedures:

20 **A. Processing the Search Sites and Securing the Data.**

21 a. The search team will conduct an initial review of any digital devices
22 or other electronic storage media located on the SUBJECT's person or in his immediate
23 control, as described in Attachment A that are capable of containing data or items that fall
24 within the scope of Attachment B to this Affidavit, to determine if it is possible to secure
25 the electronically stored information ("ESI") contained on these devices onsite in a
26 reasonable amount of time and without jeopardizing the ability to accurately preserve the
27 data.

28 b. If, based on their training and experience, and the resources
available to them at the search site, the search team determines it is not practical to make
an on-site image within a reasonable amount of time and without jeopardizing the ability
to accurately preserve the data, then the digital devices or other electronic storage media

1 will be seized and transported to an appropriate law enforcement laboratory to be
2 forensically copied ("imaged") and reviewed.

3 c. In order to examine the ESI in a forensically sound manner, law
4 enforcement personnel with appropriate expertise will attempt to produce a complete
5 forensic image, if possible and appropriate, of any digital device or other electronic
6 storage media that is capable of containing data or items that fall within the scope of
7 Attachment B to this Affidavit.² In addition, appropriately trained personnel may search
8 for and attempt to recover deleted, hidden, or encrypted data to determine whether the
9 data fall within the list of items to be seized pursuant to the warrant. In order to search
10 fully for the items identified in the warrant, law enforcement personnel, which may
11 include investigative agents, may then examine all of the data contained in the forensic
12 image/s and/or on the digital devices to view their precise contents and determine
13 whether the data fall within the list of items to be seized pursuant to the warrant.

14 d. The search techniques that will be used will be only those
15 methodologies, techniques and protocols as may reasonably be expected to find, identify,
16 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to
17 the warrant.

18 e. A forensic image may be created of either a physical drive or a
19 logical drive. A physical drive is the actual physical hard drive that may be found in a
20 typical computer. When law enforcement creates a forensic image of a physical drive,
21 the image will contain every bit and byte on the physical drive. A logical drive, also
22 known as a partition, is a dedicated area on a physical drive that may have a drive letter
23 assigned (for example the c: and d: drives on a computer that actually contains only one
24 physical hard drive). Therefore, creating an image of a logical drive does not include
25 every bit and byte on the physical drive. Law enforcement will only create an image of
26 physical or logical drives physically present on or within the subject device. Creating an
27 image of the devices located at the search locations described in Attachment A will not
28 result in access to any data physically located elsewhere. However, digital devices or
other electronic storage media at the search locations described in Attachment A that

² The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

1 have previously connected to devices at other locations may contain data from those
2 other locations.

3 f. If, after conducting its examination, law enforcement personnel
4 determine that any digital device is an instrumentality of the criminal offenses referenced
5 above, the government may retain that device during the pendency of the case as
6 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
7 the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel
8 determine that a device was not an instrumentality of the criminal offenses referenced
9 above, it shall be returned to the person/entity from whom it was seized within 60 days of
10 the issuance of the warrant, unless the government seeks and obtains authorization from
11 the court for its retention.

12 **B. Items to be Seized**

13 a. In order to search for ESI that falls within the list of items to be
14 seized pursuant to Attachment B to this Affidavit, law enforcement personnel will seize
15 and search the following items (heretofore and hereinafter referred to as "digital
16 devices"), subject to the procedures set forth above:

17 i. Any digital device capable of being used to commit, further,
18 or store evidence of the offense(s) listed above;

19 ii. Any digital device used to facilitate the transmission,
20 creation, display, encoding, or storage of data, including word processing equipment,
21 modems, docking stations, monitors, printers, cameras, encryption devices, and optical
22 scanners;

23 iii. Any magnetic, electronic, or optical storage device capable of
24 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
25 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
26 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

27 iv. Any documentation, operating logs and reference manuals
28 regarding the operation of the digital device, or software;

v. Any applications, utility programs, compilers, interpreters,
and other software used to facilitate direct or indirect communication with the device
hardware, or ESI to be searched;

vi. Any physical keys, encryption devices, dongles and similar
physical items that are necessary to gain access to the digital device, or ESI; and

1 vii. Any passwords, password files, test keys, encryption codes or
2 other information necessary to access the digital device or ESI.

3 **B. Searching the Forensic Images.**

4 a. Searching the forensic images for the items described in Attachment
5 B may require a range of data analysis techniques. In some cases, it is possible for agents
6 and analysts to conduct carefully targeted searches that can locate evidence without
7 requiring a time-consuming manual search through unrelated materials that may be
8 commingled with criminal evidence. In other cases, however, such techniques may not
9 yield the evidence described in the warrant, and law enforcement may need to conduct
10 more extensive searches to locate evidence that falls within the scope of the warrant. The
11 search techniques that will be used will be only those methodologies, techniques and
12 protocols as may reasonably be expected to find, identify, segregate and/or duplicate the
13 items authorized to be seized pursuant to Attachment B to this affidavit. Those
14 techniques, however, may necessarily expose many or all parts of a hard drive to human
15 inspection in order to determine whether it contains evidence described by the warrant.

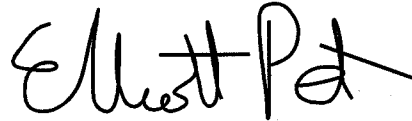
16 b. These methodologies, techniques and protocols may include the use
17 of a "hash value" library to exclude normal operating system files that do not need to be
18 further searched. Agents may also utilize hash values to exclude certain known files,
19 such as the operating system and other routine software, from the search results.
20 However, because the evidence I am seeking does not have particular known hash values,
21 agents will not be able to use any type of hash value library to locate the items identified
22 in Attachment B.

23 **REQUEST FOR SEALING**

24 38. It is respectfully requested that this Court issue an order sealing, as
25 described in the Motion to Seal submitted with this warrant, all papers submitted in
26 support of this application, including the application, affidavit and search warrant. I
27 believe that sealing this document is necessary because the items and information to be
28 seized are relevant to an ongoing investigation and disclosure of the search warrant, this
affidavit, and/or this application and the attachments thereto will jeopardize the progress
of the investigation. Disclosure of these materials would give the target of the
investigation an opportunity to destroy evidence, change patterns of behavior, notify
confederates, or flee from prosecution.

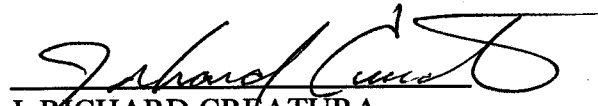
CONCLUSION

39. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of the crimes of 18 U.S.C. §§ 1030 (unauthorized damage to a protected computer) and 1343 (wire fraud) are located on devices on the person of the SUBJECT or in his immediate control, as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices or other electronic storage media found on the SUBJECT. I therefore request that the court issue a warrant authorizing a search of the SUBJECT, as well as any digital devices and electronic storage media located in his control, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.



Elliott Peterson, Affiant
Special Agent
Federal Bureau of Investigation

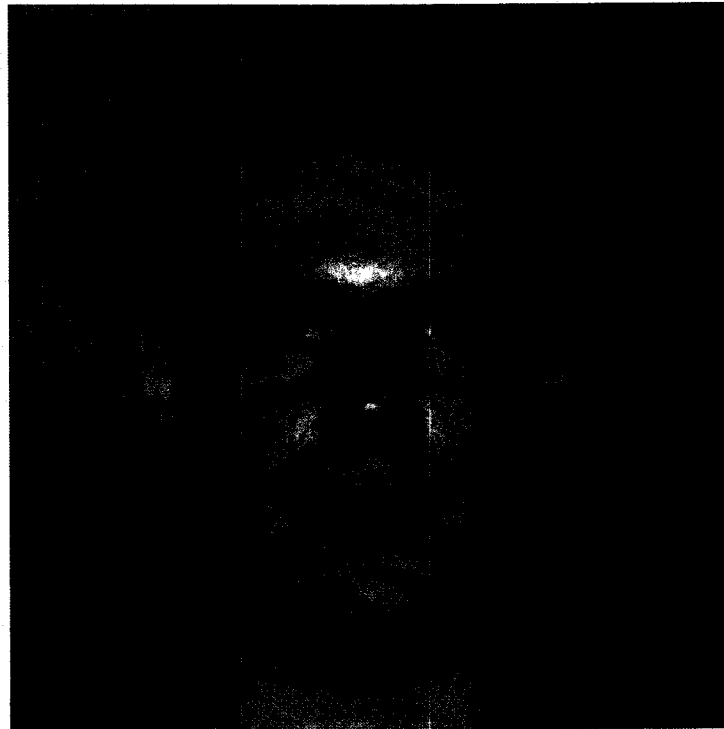
The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on this 26 day of July, 2018.



J. RICHARD CREATURA
United States Magistrate Judge

ATTACHMENT A

The property to be searched is the person of the **SUBJECT, Kenneth Currin Schuchman, within the Western District of Washington**, further described as a white adult male, DOB 04-27-1998, height 6'01", weight 200 pounds, and any digital devices or other electronic storage media found in his immediate possession or control.



ATTACHMENT B**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, laptop computers, cell phones, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 1030 (unauthorized damage to a protected computer) and 1343 (wire fraud):

1. All records relating to violations of 18 U.S.C. §§ 1030 (unauthorized damage to a protected computer) and 1343 (wire fraud) and involving the SUBJECT since July 2016, including:
 - a. Records related to Distributed Denial of Service (DDOS) attack(s);
 - b. Records related to the creation, development, operation, maintenance, purchase, or sale of a botnet(s);
 - c. Records and information relating to malicious software;
 - d. Records regarding the identity or location of co-conspirator(s);
 - e. Communications among co-conspirators;
 - f. Records regarding the identity or location of victim(s);
 - g. Records and things related to the use of Internet Protocol addresses 185.188.206.99, 45.32.238.229, 208.78.71.34, as well as the domains nexusiotsolutions.com, nexuszeta.com, and zetastress.net;
 - h. Evidence of communications with devices associated with criminal botnets, including:
 - i. routers, modems, and network equipment used to connect computers to the Internet;
 - ii. records of Internet Protocol addresses used;
 - iii. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. Any digital devices³ or other electronic storage media⁴ and/or their components that were or may have been used as a means to commit the offenses described on the warrant, including violations of 18 U.S.C. § 1030, which include:

- a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;
- b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;
- c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;
- d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;
- e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;
- f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and
- g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

³ "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

⁴ Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 3. For any digital device or other electronic storage media whose seizure is
 2 otherwise authorized in this warrant, or upon which electronically stored
 3 information that is called for by this warrant may be contained, or that may
 4 contain things otherwise called for by this warrant:

- 5 a. evidence of who used, owned, or controlled the digital device or
 6 other electronic storage media at the time the things described in this
 7 warrant were created, edited, or deleted, such as logs, registry
 8 entries, configuration files, saved usernames and passwords,
 9 documents, browsing history, user profiles, email, email contacts,
 10 "chat," instant messaging logs, photographs, and correspondence;
- 11 b. evidence of software that would allow others to control the digital
 12 device or other electronic storage media, such as viruses, Trojan
 13 horses, and other forms of malicious software, as well as evidence of
 14 the presence or absence of security software designed to detect
 15 malicious software;
- 16 c. evidence of the lack of such malicious software;
- 17 d. evidence of the attachment to the digital device of other storage
 18 devices or similar containers for electronic evidence;
- 19 e. evidence of counter-forensic programs (and associated data) that are
 20 designed to eliminate data from the digital device or other electronic
 21 storage media;
- 22 f. evidence of the times the digital device or other electronic storage
 23 media was used;
- 24 g. passwords, encryption keys, and other access devices that may be
 25 necessary to access the digital device or other electronic storage
 26 media;
- 27 h. documentation and manuals that may be necessary to access the
 28 digital device or other electronic storage media or to conduct a
 forensic examination of the digital device or other electronic storage
 media;
- i. contextual information necessary to understand the evidence
 described in this attachment.

24 SEARCH TECHNIQUES

25 In accordance with the information in this Affidavit, law enforcement personnel
 26 will execute the search of digital devices seized pursuant to this warrant as follows:

- 27 a. The search team will conduct an initial review of any digital devices
 28 or other electronic storage media located on the SUBJECT's person or in his immediate
 control, as described in Attachment A that are capable of containing data or items that fall

1 within the scope of Attachment B to this Affidavit, to determine if it is possible to secure
2 the electronically stored information ("ESI") contained on these devices onsite in a
3 reasonable amount of time and without jeopardizing the ability to accurately preserve the
4 data.

5 b. If, based on their training and experience, and the resources
6 available to them at the search site, the search team determines it is not practical to make
7 an on-site image within a reasonable amount of time and without jeopardizing the ability
8 to accurately preserve the data, then the digital devices or other electronic storage media
9 will be seized and transported to an appropriate law enforcement laboratory to be
10 forensically copied ("imaged") and reviewed.

11 c. In order to examine the ESI in a forensically sound manner, law
12 enforcement personnel with appropriate expertise will attempt to produce a complete
13 forensic image, if possible and appropriate, of any digital device or other electronic
14 storage media that is capable of containing data or items that fall within the scope of
15 Attachment B to this Affidavit.⁵ In addition, appropriately trained personnel may search
16 for and attempt to recover deleted, hidden, or encrypted data to determine whether the
17 data fall within the list of items to be seized pursuant to the warrant. In order to search
18 fully for the items identified in the warrant, law enforcement personnel, which may
19 include investigative agents, may then examine all of the data contained in the forensic
20 image/s and/or on the digital devices to view their precise contents and determine
21 whether the data fall within the list of items to be seized pursuant to the warrant.

22 d. The search techniques that will be used will be only those
23 methodologies, techniques and protocols as may reasonably be expected to find, identify,
24 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to
25 the warrant.

26 e. A forensic image may be created of either a physical drive or a
27 logical drive. A physical drive is the actual physical hard drive that may be found in a
28 typical computer. When law enforcement creates a forensic image of a physical drive,
the image will contain every bit and byte on the physical drive. A logical drive, also

⁵ The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

1 known as a partition, is a dedicated area on a physical drive that may have a drive letter
2 assigned (for example the c: and d: drives on a computer that actually contains only one
3 physical hard drive). Therefore, creating an image of a logical drive does not include
4 every bit and byte on the physical drive. Law enforcement will only create an image of
5 physical or logical drives physically present on or within the subject device. Creating an
6 image of the devices located at the search locations described in Attachment A will not
7 result in access to any data physically located elsewhere. However, digital devices or
8 other electronic storage media at the search locations described in Attachment A that
9 have previously connected to devices at other locations may contain data from those
10 other locations.

11 f. If, after conducting its examination, law enforcement personnel
12 determine that any digital device is an instrumentality of the criminal offenses referenced
13 above, the government may retain that device during the pendency of the case as
14 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
15 the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel
16 determine that a device was not an instrumentality of the criminal offenses referenced
17 above, it shall be returned to the person/entity from whom it was seized within 60 days of
18 the issuance of the warrant, unless the government seeks and obtains authorization from
19 the court for its retention.

20 In order to search for ESI that falls within the list of items to be seized pursuant to
21 Attachment B to this Affidavit, law enforcement personnel will seize and search the
22 following items (heretofore and hereinafter referred to as "digital devices"), subject to the
23 procedures set forth above:

24 a. Any digital device capable of being used to commit, further, or store
25 evidence of the offense(s) listed above;

26 b. Any digital device used to facilitate the transmission, creation,
27 display, encoding, or storage of data, including word processing equipment, modems,
28 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

29 c. Any magnetic, electronic, or optical storage device capable of
30 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
31 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
32 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

33 d. Any documentation, operating logs and reference manuals regarding
34 the operation of the digital device, or software;

1 e. Any applications, utility programs, compilers, interpreters, and other
2 software used to facilitate direct or indirect communication with the device hardware, or
3 ESI to be searched;

4 f. Any physical keys, encryption devices, dongles and similar physical
5 items that are necessary to gain access to the digital device, or ESI; and

6 g. Any passwords, password files, test keys, encryption codes or other
7 information necessary to access the digital device or ESI.

8 **The seizure of digital devices or other electronic storage media and/or their**
9 **components, as set forth herein, is specifically authorized by this search warrant, not**
10 **only to the extent that such digital devices or other electronic storage media constitute**
11 **instrumentalities of the criminal activity described above, but also for the purpose of**
12 **conducting off-site examinations of their contents for evidence, instrumentalities, or**
13 **fruits of the aforementioned crimes.**
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28